



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|----------------------|---------------------|------------------|
| 09/754,813 | 01/04/2001 | Jing Min Xu | JP919990266US1 | 3476 |

7590 01/31/2003

Louis P. Herzberg
IBM CORPORATION
INTELLECTUAL PROPERTY LAW DEPT.
P.O. BOX 218
YORKTOWN HEIGHTS, NY 10598

EXAMINER

CHEN, CHONGSHAN

| | |
|----------|--------------|
| ART UNIT | PAPER NUMBER |
|----------|--------------|

2172

DATE MAILED: 01/31/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/754,813

Applicant(s)

XU ET AL.

Examiner

Chongshan Chen

Art Unit

2172

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-20 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☒ Claim(s) 1-20 is/are rejected.
- 7) ☒ Claim(s) 18-20 is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on ____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on ____ is: a) ☐ approved b) ☐ disapproved by the Examiner.
- If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

- 13) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. ____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
- a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) ____.
- 4) ☐ Interview Summary (PTO-413) Paper No(s). ____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other:

DETAILED ACTION

Claim Objections

1. Claims 18-20 are objected to because of the following informalities:

Claims 18-20 should depend on claim 17 not claim 18.

Appropriate correction is required.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless:

(e) the invention was described in

(1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or

(2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1-20 are rejected under 35 U.S.C. 102(e) as being anticipated by Aucsmith [6,134,551].

Regarding to claim 1, Aucsmith discloses a system comprising:

a plurality of certificate authorities (CAs) in which each CA maintains and distributes digital certificates revoked by itself in the form of a certificate revocation list (CRL), and

Art Unit: 2172

different CAs may use different CRL distribution mechanisms (Aucsmith, Fig. 2, col. 3, lines 14-22);

a plurality of CRL databases for storing the consolidated CRLs from multiple CRL retrieval agents and/or the replications of CRLs (Aucsmith, Fig. 2, 222 – “Invalidity Database”, 218 – “Local Invalidity Cache”); and

a CRL access user interface for providing a uniform set of APIs for user's accessing the CRLs CRL databases, said system enabling consolidation and access of the certificate revocation list (CRL) (Aucsmith, 23-52, “the client 210 performs a lookup in a local invalidity cache 218. ... the client may perform an invalidity confirmation process wherein the client communicates with the server 220 and requests a lookup to confirm the key’s membership in invalidity database 222”).

Regarding to claim 2, Aucsmith teaches all the claimed subject matters as discussed in claim 1, and further discloses said plurality of CRL databases include a central CRL database and a plurality of CRL replication databases, said central CRL database for storing the consolidated CRLs from the multiple CRL retrieval agents, and said plurality of CRL replication databases for storing the replications of the CRLs of the central CRL database (Aucsmith, Fig. 2, col. 3, lines 14-67).

Regarding to claim 3, Aucsmith teaches all the claimed subject matters as discussed in claim 1, and further discloses CRL retrieval agents include a LDAP/CRL retrieval agent, for periodically retrieving CRLs from specified LDAP servers and updating the CRL databases (Aucsmith, col. 3, lines 53-67, “Local invalidity cache is a bloom filter of all the invalid keys in the database 222. ... Any of the bloom filter vectors, coefficients, and prime key values may be

Art Unit: 2172

downloaded from server 220 by client 210 upon demand, at regular intervals, or other defined intervals according to the established protocol". The established protocol inherently includes LDAP server).

Regarding to claim 4, Aucsmith teaches all the claimed subject matters as discussed in claim 1, and further discloses CRL retrieval agents include a HTTP/CRL retrieval agent, for periodically retrieving CRLs from specified HTTP servers and updating the CRL database (Aucsmith, col. 3, lines 53-67, "Local invalidity cache is a bloom filter of all the invalid keys in the database 222. ... Any of the bloom filter vectors, coefficients, and prime key values may be downloaded from server 220 by client 210 upon demand, at regular intervals, or other defined intervals according to the established protocol". The established protocol inherently includes HTTP server).

Regarding to claim 5, Aucsmith teaches all the claimed subject matters as discussed in claim 1, and further discloses CRL retrieval agents include a RFC1424/CRL retrieval agents, for periodically sending RFC1424/CRL retrieval request and receiving CRL retrieval reply (Aucsmith, col. 3, lines 53-67).

Regarding to claim 6, Aucsmith teaches all the claimed subject matters as discussed in claim 1, and further discloses CRL retrieval agents include a HTTP receiver agent triggered by a HTTP request, said HTTP receiver agent verifies an authorization of the requester, if successful, said agent stores each transmitted CRL in the CRL databases (Aucsmith, col. 7, lines 12-42).

Regarding to claim 7, Aucsmith teaches all the claimed subject matters as discussed in claim 1, and further discloses CRL retrieval agents further verifies the integrity and the authenticity of the retrieved CRLs (Aucsmith, col. 3, lines 35-40).

Regarding to claim 8, Aucsmith teaches all the claimed subject matters as discussed in claim 1, and further discloses a particular replication architecture is used among said plurality of CRL databases in order to maintain database consistency (Aucsmith, col. 3, lines 63-67).

Regarding to claim 9, Aucsmith teaches all the claimed subject matters as discussed in claim 2, and further discloses a sub-and-spoke replication architecture is used among said central CRL database and said plurality of CRL replication databases (Aucsmith, Fig. 2 & 5).

Regarding to claim 10, Aucsmith teaches all the claimed subject matters as discussed in claim 1, and further discloses system is also adapted for consolidating and accessing at least one kind of black list (Aucsmith, col. 3, lines 14-22).

Regarding to claim 11, Aucsmith discloses in a secure network implemented by digital certificates, a method for certificate revocation list (CRL) consolidation and access, wherein a plurality of certificate authorities (CAs) maintain and distribute the digital certificates revoked by themselves in the form of CRLs, and different CAs may use different CRL distribution mechanisms, said method comprising the steps of:

creating a plurality of CRL retrieval agents based on the CRL distribution mechanisms of CAs, for consolidating the CRLs from multiple CAs; storing the consolidated CRLs from multiple CRL retrieval agents or the replications of CRLs into a plurality of CRL databases (Aucsmith, col. 14-34); and

accessing the CRLs from the CRL databases by a uniform set of APIs (Aucsmith, col. 3, lines 35-45, "perform an invalidity confirmation process wherein the client communicates with the server 220 and requests a lookup to confirm the key's membership in invalidity database 222").

Regarding to claim 12, Aucsmith teaches all the claimed subject matters as discussed in claim 11, and further discloses CRL databases include a central CRL database and a plurality of CRL replication database, said central CRL database for storing the consolidated CRLs from multiple CRL retrieval agents and said plurality of CRL replication database for storing the replications of the CRLs of the central database (Aucsmith, Fig. 2, 222 – “Invalidity Database”, 218 – “Local Invalidity Cache”, col. 3, lines 53-67).

Regarding to claim 13, Aucsmith teaches all the claimed subject matters as discussed in claim 11, and further discloses consolidating and accessing all kinds of black lists (Aucsmith, col. 3, lines 14-22).

Regarding to claim 14, Aucsmith teaches all the claimed subject matters as discussed in claim 11, and further discloses an article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing certificate revocation list (CRL) consolidation and access, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 11 (Aucsmith, Fig. 3, col. 4, lines 12-67).

Regarding to claim 15, Aucsmith teaches all the claimed subject matters as discussed in claim 11, and further discloses a computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing certificate revocation list (CRL) consolidation and access, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the steps of claim 11 (Aucsmith, Fig. 3, col. 4, lines 12-67).

Regarding to claim 16, Aucsmith teaches all the claimed subject matters as discussed in claim 11, and further discloses a program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for certificate revocation list (CRL) consolidation and access, said method steps comprising the steps of claim 11 (Aucsmith, Fig. 3, col. 4, lines 12-67).

Regarding to claim 17, Aucsmith discloses a method comprising:

employing a secure network implemented by digital certificates for certificate revocation list (CRL) consolidation and access, with a plurality of certificate authorities (CAs) maintaining and distributing the digital certificates revoked by themselves in the form of CRLs, wherein different CAs may use different CRL distribution mechanisms, including the steps of: creating a plurality of CRL retrieval agents based on the CRL distribution mechanisms of CAs, for consolidating the CRLs from multiple CAs; storing the consolidated CRLs from multiple CRL retrieval agents or the replications of CRLs into a plurality of CRL databases (Aucsmith, col. 14-34); and

accessing the CRLs from the CRL databases by a uniform set of APIs (Aucsmith, col. 3, lines 35-45, “perform an invalidity confirmation process wherein the client communicates with the server 220 and requests a lookup to confirm the key’s membership in invalidity database 222”).

Regarding to claim 18, Aucsmith teaches all the claimed subject matters as discussed in claim 17, and further discloses a program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for

Art Unit: 2172

certificate revocation list (CRL) consolidation and access, said method steps comprising the steps of claim 17 (Aucsmith, Fig. 3, col. 4, lines 12-67).

Regarding to claim 19, Aucsmith teaches all the claimed subject matters as discussed in claim 17, and further discloses an article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing certificate revocation list (CRL) consolidation and access, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 17 (Aucsmith, Fig. 3, col. 4, lines 12-67).

Regarding to claim 20, Aucsmith teaches all the claimed subject matters as discussed in claim 17, and further discloses a computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing certificate revocation list (CRL) consolidation and access, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the steps of claim 17 (Aucsmith, Fig. 3, col. 4, lines 12-67).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Chongshan Chen whose telephone number is (703) 305-8319. The examiner can normally be reached on Monday - Friday (8:00 am - 4:30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y Vu can be reached on (703)305-4393. The fax phone numbers for the

Application/Control Number: 09/754,813

Page 9


Art Unit: 2172

organization where this application or proceeding is assigned are (703) 746-7239 for regular communications and (703) 746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703)305-3900.

CC

January 24, 2003


SHAHID AL ALAM
PATENT EXAMINER